IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:
Jean Renard Ward

Art Unit: 2139

Confirmation No.: 1705

Application No.: 10/734,614

Filed: December 12, 2003

**VIA ELECTRONIC FILING**

For: PROTECTION OF IDENTIFICATION DOCUMENTS USING OPEN CRYPTOGRAPHY

Examiner: J. Turchen

Date: July 29, 2008

**PRE-APPEAL BRIEF REQUEST FOR REVIEW**

Sir:

Appellant requests review of the rejection in the above-identified application. No amendment is being filed with this request. (This request is proper since the claims have been twice rejected.)

This request is being filed with a Notice of Appeal.

The review is requested for the reasons stated on the attached sheets. (No more than 5 pages are provided.)

Respectfully submitted,

Date: July 29, 2008

DIGIMARC CORPORATION

CUSTOMER NUMBER 23735

Phone: 503-469-4800
FAX: 503-469-4777

By: /Steven W. Stewart, Reg. No. 45,133/
Steven W. Stewart
Registration No. 45,133

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:
Jean Renard Ward

Art Unit: 2139

Confirmation No.: 1705

Application No.: 10/734,614

Filed: December 12, 2003

**VIA ELECTRONIC FILING**

For: PROTECTION OF IDENTIFICATION DOCUMENTS USING OPEN CRYPTOGRAPHY

Examiner: J. Turchen

Date: July 29, 2008

## REASONS FOR PRE-APPEAL BRIEF REQUEST FOR REVIEW

*Introduction*

On appeal the rejection of claims 1-32 will be reversed for at least the reasons noted below:

*Claim 1*

Claim 1 recites – in combination with other features – an identification document including a security feature printed on a surface of the identification document in a two-dimensional encoded symbology. The security feature includes a first set of information; the first set of information includes an unencrypted form. So, the security feature of claim 1 is in an encode symbology, e.g., such as a barcode, 2D-barcode, data glyph, maxicode, PDF 417, DataMatrix, and QR Code. But at least a first set of information in this encoded symbology is unencrypted.

Chow *teaches away* from the claimed arrangement. See Chow at Col. 4, lines 62-67. There, Chow states that all of the information in the encoded symbology is encrypted. (This corresponds to the area depicted as item 3 in Chow's Fig. 2, below.) Having all the information encrypted *teaches away* from the arrangement recited in claim 1. See KSR, citing Untied States v. Adam, 383 US 39 (1966), stating in part that, "the Court relied upon the corollary principle that when the prior art teaches away from combining certain known elements, discovery of a successful means of combining them is more likely to be nonobvious."

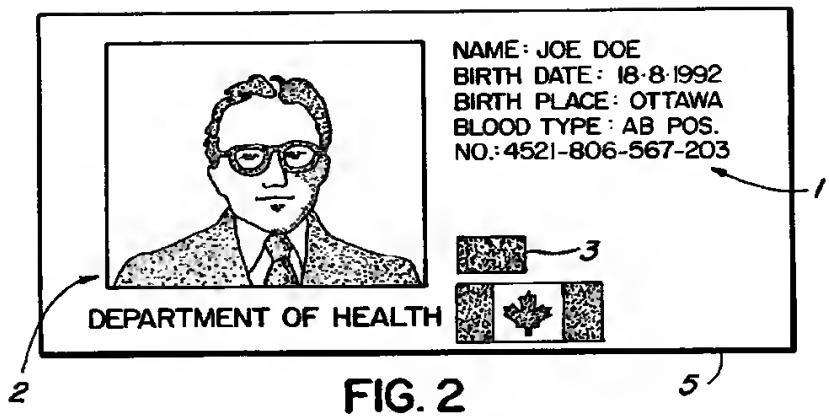


FIG. 2

The Office Action then cites to area 1 as providing an unencrypted form of the first information. See the Office Action, page 2, last 5 lines. But area 1 (plain text) is not part of the encoded symbology (area 3) as required by claim 1. That is, the first set of information of claim 1 is carried by the encoded symbology.

The rejection of claim 1 will be reversed on appeal.

*Claim 9*

Claim 9 recites that a cryptographic measure includes at least a first digital signature and a second digital signature. The first digital signature corresponds to a first stage of a document fabrication process, and the second digital signature corresponds to a second stage of the document fabrication process.

The Office Action acknowledges that Chen and Chow are deficient in this regard. Please see the Office Action on page 6, last paragraph. So the Office Action turns to Manabe at paragraph 69 to remedy the deficiencies.

We disagree with this analysis. While the Manabe passage (paragraph 69) discusses inserting discrimination information for a printing person (or control system) via a watermark, it says nothing of including a first digital signature corresponding to a first stage of a document fabrication process, and a second digital signature corresponding to a second stage of the document fabrication process.

The Office Action overstates the teachings of the applied art. As such, the rejection of claim 9 will be reversed on appeal.

*Claim 13*

Claim 13 recites a second set of information (included in the cryptographic measure) having a document inventory number. The inventory number is conveyed by a machine-readable code carried by the identification document.

The Office Action – without any justification, foundation or explanation – states that the inventory number is merely an identification number. See the Office Action, page 6, first paragraph. But claim language cannot simply be rewritten to suit a particular rejection. In the instant case, however, the Examiner has replaced the term "inventory" with the term "identification".

This approach ignores the historical use of an identification number, the ID fabrication process, and varied components of ID document fabrication inventory.

Moreover, the stated reasons of obviousness (obvious to move the identification number from section to section 2 using either an overlay or a displaying the ID number at the side of the picture) does nothing to address an "inventory" number vs. an identification number.

The rejection of claim 13 will be reversed on appeal.

*Claim 15*

Claim 15 recites – in combination with other features – determining *construction materials, equipment or processing* details of the identification document *from at least a cryptographic signature.*

The Office Action cites Manabe at paragraph 69 as meeting this feature.

We disagree. While that passage discusses inserting discrimination information for a printing person (or control system) via a watermark, it says nothing of determining *construction materials, equipment or processing* details of the identification document *from at least a cryptographic signature.*

The rejection of claim 15 will be reversed on appeal.

*Claim 16*

Claim 16 recites that the machine-readable format (of claim 15) comprises digital watermarking.

One of ordinary skill in the art will appreciate that in the context of the specification, the term "digital watermarking" implies data hiding or steganography. For example, the specification defines the term digital watermark – for this application – as a form of steganography. See paragraph [0106]: ("Digital watermarking technology, a form of steganography, encompasses a great variety of techniques by which plural bits of digital data are hidden in some other object, preferably without leaving human-apparent evidence of alteration.").

A "steganographic" definition is buttressed by the cannon of claim differentiation in view of claim 17. Claim 17 recites: "The method of claim 15, wherein the machine-readable format comprises a two-dimensional symbology." Claims 16 and 17 claim different aspects of the invention. Thus, if a "two-dimensional symbology" is expressly recited in claim 17, then claim 16's "digital watermarking" should be interpreted as meaning something different.

The rejection of claim 16 will be reversed on appeal.

*Claim 21*

Claim 21 recites – in combination with other features – that a cryptographic signature comprises a date indicator. The act of determining includes determining whether the date indicator corresponds with an untrusted – *but not expired* – date. Thus, the untrusted date is not an expired date.

The Office Action cites to page 33 of "How Digital Certificates Work" as meeting these features. See the Office Action, page 10, last four lines.

We disagree with that analysis.

The cited page 33 says nothing of a date indicator corresponding to an untrusted – *but not expired* – date. In fact, page 33 offers contrary advice: "Although CertificateHold allow a certificate to be unrevoked, it is not recommended to place a hold on a certificate, *as it becomes difficult to determine if a certificate was valid for a specific time*." (*emphasis added*).

The rejection of claim 21 will be reversed on appeal.

*Claim 27*

Claim 27 recites – in combination with other features – a method to determine whether an identification document *is fabricated on authorized equipment* but is issued in an unauthorized manner.

The Office Action does not address this feature (among others), nor is the applied art understood to render such features obvious.

The rejection of claim 27 will be reversed on appeal.

*Claim 29*

Claim 29 recites a method including: *randomly or pseudo-randomly selecting a unique serial number*; associating the unique serial number and fabrication details in a data record; providing the unique serial number on the identification document; and issuing the identification document.

The Office Action takes official notice that pseudo-random and random number generation were well known in the art at the time of the invention. See the Office Action, page 12, last full paragraph. We do not dispute that such random generation techniques were known. We do dispute, however, whether such techniques would have been employed in the manner claimed to select a unique serial number.

In this regard, the Office Action fails to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements as in claim 29. This cuts against the advice in KSR v. Teleflex, at 15. Indeed, the Office Action lacks any discussion of the apparent reasons to combine known elements in the fashion claimed, including a detailed explanation of the effects of demands known to the design community or present in the marketplace and the background knowledge possessed by a person having ordinary skill in the art. See KSR, at 14.

The rejection of claim 29 will be reversed on appeal.

Respectfully submitted,

Date: July 29, 2008

DIGIMARC CORPORATION

CUSTOMER NUMBER 23735

By: /Steven W. Stewart, Reg. No. 45,133/
Steven W. Stewart
Registration No. 45,133

Phone: 503-469-4800
FAX: 503-469-4777